



06-14-05

IPW
AF-5

TRANSMITTAL OF APPEAL BRIEF			Docket No. 56728/P002US/10005779
In re Application of: Mohammad Husain et al.			
Application No. 09/588,453-Conf. #9205	Filing Date June 6, 2000	Examiner B. E. Lanier	Group Art Unit 2132
Invention: SYSTEM AND METHOD FOR SECURE AUTHENTICATION OF A SUBSCRIBER OF NETWORK SERVICES			

TO THE COMMISSIONER OF PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: April 12, 2005

The fee for filing this Appeal Brief is \$ 250.00

☐ Large Entity ☒ Small Entity

☐ A petition for extension of time is also enclosed.

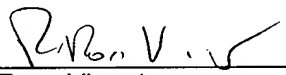
The fee for the extension of time is _____

☐ A check in the amount of _____ is enclosed.

☒ Charge the amount of the fee to Deposit Account No. \$250.00
This sheet is submitted in duplicate.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. 06-2380
This sheet is submitted in duplicate.


R. Ross Viguet
Attorney Reg. No. : 42,203
FULBRIGHT & JAWORSKI L.L.P.
2200 Ross Avenue, Suite 2800
Dallas, Texas 75201-2784
(214) 855-8185

Dated: June 13, 2005

Appeal Brief Transmittal

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV482707743, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

Dated: June 13, 2005

Signature:  (Lisa deCordova)



Docket No.: 56728/P002US/10005779
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Mohammad Husain et al.

Application No.: 09/588,453

Confirmation No.: 9205

Filed: June 6, 2000

Art Unit: 2132

For: SYSTEM AND METHOD FOR SECURE
AUTHENTICATION OF A SUBSCRIBER OF
NETWORK SERVICES

Examiner: B. E. Lanier

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This brief is filed in furtherance of the Notice of Appeal filed in this case on
April 12, 2005.

The fees required under § 41.20(b)(2) are dealt with in the accompanying
TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R.
§ 41.37 and M.P.E.P. § 1206:

- | | |
|-------|---|
| I. | Real Party In Interest |
| II | Related Appeals and Interferences |
| III. | Status of Claims |
| IV. | Status of Amendments |
| V. | Summary of Claimed Subject Matter |
| VI. | Grounds of Rejection to be Reviewed on Appeal |
| VII. | Argument |
| VIII. | Claims |
| IX. | Evidence |
| X. | Related Proceedings |

06/15/2005 MAHMED1 00000047 062380 09588453

01 FC:2402 250.00 DA

25538409.1

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

COMMERCIANT, L.P.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 50 claims pending in application.

B. Current Status of Claims

1. Claims canceled: 42-47 and 51-55
2. Claims withdrawn from consideration but not canceled: None
3. Claims pending: 1-41, 48-50, and 56-61
4. Claims allowed: None
5. Claims rejected: 1-41, 48-50, and 56-61

C. Claims On Appeal

The claims on appeal are claims 1-41, 48-50, and 56-61

IV. STATUS OF AMENDMENTS

No amendments were made in the response after final, dated March 7, 2005. The claims on appeal (as listed in section VIII) are the claims presented in the amendment, June 10, 2004.

V. SUMMARY OF CLAIMED SUBJECT MATTER

An embodiment provides a method for activating a subscriber account for providing a network service (page 9, lines 1-4, Figure 1). The method according to an embodiment comprises receiving initial information from a subscriber (page 9, lines 10-20, Figure 1, box 11), storing the received information (page 6, lines 5-6), providing a transaction processing device to the subscriber (page 10, lines 13-16, Figure 1, box 13), receiving captured information from the subscriber through the transaction processing device (page 12, line 17, through page 13, line 2, page 15, lines 1-9, Figure 1, box 14), utilizing the captured information to receive verifying information about the subscriber (page 16, lines 5-16, Figure 1, box 15), and comparing the verifying information with the initial information to authenticate the subscriber (page 16, lines 16-19, Figure 1, box 15).

The captured information is information provided to the subscriber by a third party certifying authority according to further embodiments (page 12, lines 21-26).

The captured information is information that has not been previously provided to the provider of the subscriber account by the subscriber according to further embodiments (page 13, lines 8-13).

The method according to embodiments further comprises providing at least a portion of the decrypted information to a third party server (page 16, lines 5-16, Figure 1, box 15), and receiving the verifying information from the third party server in response to providing the decrypted information to the third party server (page 16, lines 12-16).

The method according to embodiments further comprises retrieving, by the subscriber account provider, verifying information from the remote server, wherein the verifying information had been previously retrieved by the subscriber account provider from a third party server (page 18, lines 16-20).

An embodiment provides a method for electronic authentication of a subscriber requesting a subscriber account for providing a payment processing service (page 9, lines 1-4, page 18, lines 26-28, Figure 1). The method according to an embodiment comprises receiving initial information from the subscriber, wherein the initial information is received by a payment processor (page 9, lines 8-20, Figure 1, box 11), storing the received

information in a database associated with the payment processor (page 6, lines 16-17), providing a point of sale terminal to the subscriber (page 10, lines 13-16, Figure 1, box 13), receiving by the point of sale terminal identifying information from the subscriber, wherein the identifying information is captured by the transaction processing device, wherein at least a portion of the captured information is encrypted by the point of sale terminal (page 12, line 17, through page 13, line 2, page 15, lines 1-13, Figure 1, box 14), receiving the encrypted information from the point of sale terminal via a public network (page 15, lines 19-21), decrypting the received encrypted information by the payment processor (page 15, lines 24-26), providing at least a portion of the decrypted information to a third party server (page 16, lines 5-16, Figure 1, box 15), receiving verifying information from the third party server wherein the verifying information is related to the decrypted information provided to the third party server (page 16, lines 12-16), comparing the verifying information with the initial information by the payment processor to authenticate the subscriber (page 16, lines 16-19, Figure 1, box 15), and activating the subscriber account for performing the payment processing service upon authentication of the subscriber (page 18, lines 26-28, Figure 1, box 16).

An embodiment provides a method of activating a subscriber account for providing a network service via a transaction processing device (page 9, lines 1-4, page 18, lines 26-28, Figure 1). The method according to an embodiment comprises receiving initial information from a subscriber (page 9, lines 8-20, Figure 1, box 11), storing the initial information (page 6, lines 5-6), providing the transaction processing device to the subscriber (page 10, lines 13-16, Figure 1, box 13), receiving identification information from the subscriber through the transaction processing device (page 12, line 17, through page 13, line 2, page 15, lines 1-9, Figure 1, box 14), communicating, by the transaction processing device through a network, the identification information to an authenticating server (page 15, lines 3-9), using, by the authenticating server, the identification information to obtain verifying information related to the subscriber (page 16, lines 5-16, Figure 1, box 15), and activating, by the authenticating server, the subscriber account when the verifying information is consistent with the initial information, wherein the activating enables the transaction processing device to initiate payments into the subscriber account from third parties via the network (page 18, line 26, through page 19, line 6, Figure 1, box 16).

The method according to embodiments further comprises retrieving the verifying information through a third party server (page 16, lines 12-14).

The activating according to further embodiments comprises communicating configuration information to the transaction processing device (page 19, lines 7-17).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-14, 15-35, 37, 39-41, 48-50, 56, 57, and 59-61 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,016,476 to Maes (hereinafter “Maes”).

Claims 36 and 38 are rejected under 35 U.S.C. § 103(a) are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes in view of U.S. Patent No. 6,233,577 to Ramasubramani (hereinafter “Ramasubramani”).

Claims 19 and 58 are rejected under 35 U.S.C. § 103(a) are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes in view of U.S. Patent No. 5,721,781 to Deo (hereinafter “Deo”).

Each of these rejections are submitted for review in this appeal.

VII. ARGUMENT

Rejection under 35 U.S.C. § 102(e)

Claims 1-14, 15-35, 37, 39-41, 48-50, 56, 57, and 59-61 are rejected under 35 U.S.C. § 102(e) as being anticipated by Maes.

It is well settled that to anticipate a claim, the reference must teach every element of the claim. *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, in order for a reference to be anticipatory under 35 U.S.C. § 102 with respect to a claim, “[t]he elements must be arranged as required by the claim.” *In re Bond*, 15 USPQ2d 1566 (Fed. Cir. 1990). Furthermore, in order for a reference to be anticipatory under 35 U.S.C. § 102 with respect to a claim, “[t]he identical invention must be shown in as complete detail as is contained in the . . . claim.” *Richardson v. Suzuki Motor Co.*, 9 USPQ2d

1913 (Fed. Cir. 1989). Appellant respectfully asserts that Maes does not satisfy these requirements.

Claim 1

Claim 1 is directed to a method for activating a subscriber account for providing a network service. Claim 1 recites:

- receiving initial information from a subscriber;
- storing said received information;
- providing a transaction processing device to said subscriber;
- receiving captured information from said subscriber through said transaction processing device;
- utilizing said captured information to receive verifying information about said subscriber; and
- comparing said verifying information with said initial information to authenticate said subscriber.

In the rejection of claim 1, the Examiner states that Maes discloses that a user is verified using a PIN, password, and biometric information. If the PIN, password, and biometric information are acceptable, a digital certificate is provided to the user's PDA to an account number to be written to a "smart card." Office Action, page 2.

Appellant respectfully notes that claim 1 recites three different types of information: "initial information," "captured information," and "verifying information." Each of the three different types of information are obtained in a different manner. Specifically, the initial information is received and stored and, then, a transaction processing device is provided to the subscriber. The same transaction processing device provided to the subscriber in response to the initial information is used to receive information (the captured information) from the subscriber. The captured information is not merely compared against the previously stored initial information. Instead, the captured information is then used to receive separate verifying information. The verifying information is then compared against the initial information. Upon the basis of the comparison, the subscriber is authenticated.

Maes is directed to using a personal digital assistant (PDA) to write information to a "smart card." By employing the PDA functionality, Maes enables a single smart card to be used for multiple financial accounts. To use the Maes system, a consumer initially enrolls in a service plan. The consumer identifies to the service provider all of the consumer's accounts

that the consumers wishes to manage using a “universal” card. Col. 6, lines 64-67 of Maes. The universal card operates in conjunction with a PDA. Specifically, when the user wishes to use the universal card, the user provides identifying information (e.g., a password, voice sample, biometric information, etc.). Col. 7, lines 25-31. If the identifying information matches previously stored information, a digital certificate is provided to the PDA. The digital certificate enables a specific account number to be written to the universal card for use for one or several financial transactions. Col. 7, lines 36-45. The digital certificate “contains information relating to (but not limited to) the account number of the PDA device 10, the date on which the digital certificate was authenticated and its expiration date, as well as any constraints which exist for each enrolled card.” Col. 7, lines 45-49.

Each example of verifying information (PIN, password, voice sample, biometric information) in Maes is simply compared against previously stored information. The number entered by the user is compared against the previously issued PIN. The text information entered by the user is compared against the previously stored password. The biometric information is compared against previously stored biometric information. *See* col. 7, lines 25-35 and col. 8, lines 52-61. None of the information types of Maes is used to obtain other information. Accordingly, Maes does not disclose using the three types of information in the manner recited by claim 1.

Additionally, Appellant submits that the digital certificate of Maes cannot satisfy the “verifying information” element, because the digital certificate of Maes is not compared against initial information received from the subscriber. Specifically, Maes discloses that the digital certificate contains information related to the account number of the PDA device 10, the date on which the digital certificate was authenticated and its expiration date, as well as any constraints that exist for each enrolled card. Col. 7, lines 45-50. The disclosed information in the digital certificate is related to the PDA device and the account numbers. The disclosed information is not “verifying information about said subscriber,” because the information in the digital certificate of Maes does not verify the identity of the subscriber.

Appellant respectfully submits that claim 1 is not anticipated. Claims 2-14, 15-35, 37, and 39-41 depend from claim 1 and, hence, inherit all limitations of claim 1. Claims 2-14, 15-35, 37, and 39-41 are also not anticipated.

Claim 2

Claim 2 recites “wherein said captured information is information provided to said subscriber by a third party certifying authority.” The information captured by the PDA in Maes for verification purposes is either a PIN, a password, a voice sample, or biometric information. Maes does not disclose information captured by the PDA that was provided to the user by a third party certifying authority. Accordingly, claim 2 is not anticipated.

Claim 4

Claim 4 recites “wherein said captured information is information that has not been previously provided to said provider of said subscriber account by said subscriber.” The information captured by the PDA in Maes is information that was previously provided to the service provider of Maes. For example, the service provider must have previously obtained the PIN and passwords. Additionally, the service provider also receives prior voice samples and biometric information for comparison against the received voice samples and biometric information. Accordingly, the information in Maes is not capture information not previously provided to the provider of the subscriber account by the subscriber. Accordingly, claim 4 is not anticipated.

Claims 15 and 16

Claim 15 recites “providing at least a portion of said decrypted information to a third party server; and receiving said verifying information from said third party server in response to providing said decrypted information to said third party server.” Claim 16 recites “retrieving, by said subscriber account provider, verifying information from said remote server, wherein said verifying information had been previously retrieved by said subscriber account provider from a third party server.” After the user obtains the universal card and PDA in Maes, the only information that is communicated between the PDA and the service provider is the PIN, password, voice samples, and biometric information. Specifically, all of the information in Maes is originated at the PDA by the user. None of the information communicated after the user obtains the PDA and the universal card originates from “a third party server.” Accordingly, claims 15 and 16 are not anticipated.

Claim 48

Claim 48 recites:

receiving initial information from said subscriber, wherein said initial information is received by a payment processor;
storing said received information in a database associated with said payment processor;
providing a point of sale terminal to said subscriber;
receiving by said point of sale terminal identifying information from said subscriber, wherein said identifying information is captured by said transaction processing device, wherein at least a portion of said captured information is encrypted by said point of sale terminal;
receiving said encrypted information from said point of sale terminal via a public network;
decrypting said received encrypted information by said payment processor;
providing at least a portion of said decrypted information to a third party server;
receiving verifying information from said third party server wherein said verifying information is related to said decrypted information provided to said third party server;
comparing said verifying information with said initial information by said payment processor to authenticate said subscriber.

Claim 48 authenticates a subscriber in a manner that is similar to the method of claim

1. Appellant submits that claim 48 is not anticipated at least for the reasons set forth above with respect to claim 1.

Additionally, claim 48 further recites that the initial information is received by “a payment processor.” The recited payment processor provides a “point of sale terminal” to the subscriber. Additionally, the verifying information is received from a “third party server” for comparison against “identifying information” received by the point of sale terminal. There is no basis in Maes to address these elements of claim 48.

Appellant respectfully submits that claim 48 is not anticipated. Claims 49 and 50 depend from claim 48 and, hence, inherit all limitations of claim 48. Claims 49 and 50 are likewise not anticipated.

Claim 56

Claim 56 recites

receiving initial information from a subscriber;

storing said initial information;
providing said transaction processing device to said subscriber;
receiving identification information from said subscriber through said transaction processing device;
communicating, by said transaction processing device through a network, said identification information to an authenticating server;
using, by said authenticating server, said identification information to obtain verifying information related to said subscriber; and
activating, by said authenticating server, said subscriber account when said verifying information is consistent with said initial information, wherein said activating enables said transaction processing device to initiate payments into said subscriber account from third parties via said network.

For the reasons discussed above in regard to claim 1, there is no authenticating server in Maes that (i) receives identification information from a subscriber; (ii) uses the identification information to obtain verifying information; and (iii) activates a subscriber account when the verifying information is consistent with information initially received from the subscriber. Additionally, there is no disclosure that the transaction processing device provided to the subscriber is enabled upon the “activating” to initiate payments into the subscribers account from third parties via a network. Instead, Maes merely discloses that two parties having the universal accounts can transfer funds upon mutual consent. *See* col. 14, lines 47-67 of Maes.

Claim 56 is not anticipated. Claims 57 and 59-61 depend from claim 56 and, hence, inherit all limitations of claim 56. Claims 57 and 59-61 are also not anticipated.

Claim 57

Claim 57 recites “retrieving said verifying information through a third party server.” After the user obtains the universal card and PDA in Maes, the only information that is communicated between the PDA and the service provider is the PIN, password, voice samples, and biometric information. Specifically, all of the information in Maes is originated at the PDA by the user. None of the information communicated after the user obtains the PDA and the universal card is retrieved from “a third party server.”

Claim 57 is not anticipated. Claim 58 depend from claim 57 and, hence, inherits all limitations of claim 57. Claim 58 is also not anticipated.

Claim 61

Claim 61 recites “wherein said activating comprises: communicating configuration information to said transaction processing device.” Maes merely discloses communicating digital certificates to the PDA. However, such digital certificates do not configure (“set-up”) a transaction process device as part of enabling the transaction processing device to initiate payments into a subscriber account from third parties via a network. Accordingly, claim 61 is not anticipated.

Rejections under 35 U.S.C. § 103(a)

Claims 36 and 38 are rejected under 35 U.S.C. § 103(a) are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes in view of U.S. Patent No. 6,233,577 to Ramasubramani (hereinafter “Ramasubramani”).

Claims 19 and 58 are rejected under 35 U.S.C. § 103(a) are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes in view of U.S. Patent No. 5,721,781 to Deo (hereinafter “Deo”).

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art cited must teach or suggest all the claim limitations. *In re Royka*, 180 USPQ 580 (CCPA 1974). Appellant asserts that the rejection does not satisfy these criteria.

Claims 36 and 38

Claims 36 and 38 are rejected under 35 U.S.C. § 103(a) are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes in view of Ramasubramani. Claims 36 and 38 depend from claim 1 and, hence, inherit all limitations of claim 1. For the reasons discussed above in regard to the rejection under 35 U.S.C. § 102(e), Maes does not teach or suggest each and every limitation of claim 1. Moreover, Ramasubramani is merely directed to a central digital certificate management system. *See* Abstract of Ramasubramani. Ramasubramani does not teach or suggest the limitations of claim 1. Accordingly, the

applied references (either alone or in combination) do not teach or suggest each and every limitation of claim 1. A prima facie case of obviousness has not been established for claims 36 and 38 due at least to their dependency from claim 1.

Claims 19 and 58

Claims 19 and 58 are rejected under 35 U.S.C. § 103(a) are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes in view of Deo. Claim 19 depends from claim 1 and, hence, inherits all limitations of claim 1. Claim 58 depends from claim 56 and, hence, inherits all limitations of claim 56. For the reasons discussed above in regard to the rejection under 35 U.S.C. § 102(e), Maes does not teach or suggest each and every limitation of claims 1 and 56. Moreover, Deo is merely directed to a smart card which contains a digital certificate from a certifying authority. See Abstract of Deo. Deo does not teach or suggest the limitations of claims 1 and 56. Accordingly, the applied references (either alone or in combination) do not teach or suggest each and every limitation of claims 1 and 56. A prima facie case of obviousness has not been established for claims 19 and 58 due at least to their dependency from claims 1 and 56.

Conclusion

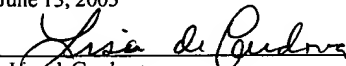
For the reasons provided herein, Appellant respectfully requests the Board to rule that the rejections of the pending claims are not proper in view of the applied references.

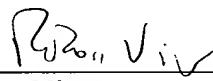
Dated: June 13, 2005

Respectfully submitted,

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as Express Mail, Airbill No. EV482707743US, in an envelope addressed to: MS Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date shown below.

June 13, 2005


Lisa deCordova

By 
R. Ross Viguet
Registration No.:
FULBRIGHT & JAWORSKI L.L.P.
2200 Ross Avenue, Suite 2800
Dallas, Texas 75201-2784
(214) 855-8185
(214) 855-8200 (Fax)

VIII. CLAIMS

1. A method for activating a subscriber account for providing a network service, comprising the steps of:

receiving initial information from a subscriber;
storing said received information;
providing a transaction processing device to said subscriber;
receiving captured information from said subscriber through said transaction processing device;
utilizing said captured information to receive verifying information about said subscriber; and
comparing said verifying information with said initial information to authenticate said subscriber.

2. The method of claim 1, wherein said captured information is information provided to said subscriber by a third party certifying authority.

3. The method of claim 1, wherein said initial information is received by a provider of said subscriber account.

4. The method of claim 3, wherein said captured information is information that has not been previously provided to said provider of said subscriber account by said subscriber.

5. The method of claim 3, wherein said receiving captured information step includes the step of:

receiving by said transaction processing device identifying information from said subscriber, wherein said identifying information is captured by said transaction processing device.

6. The method of claim 5, wherein said receiving captured information step further includes the step of:

receiving securely from said transaction processing device said captured information by a remote server associated with said provider of said subscriber account.

7. The method of claim 6, wherein at least a portion of said captured information is encrypted prior to being transmitted to said remote server over a communication network.

8. The method of claim 7, wherein said encryption is performed utilizing a private key unique to said transaction processing device.

9. The method of claim 8, wherein said captured information is further encrypted utilizing a public key of said subscriber account provider.

10. The method of claim 7, wherein said encryption is performed utilizing a public key of said subscriber account provider.

11. The method of claim 8, wherein said communications network is a public network.

12. The method of claim 11, wherein said public network is capable of TCP/IP communication.

13. The method of claim 8, wherein said utilizing said captured information step comprises the steps of:

decrypting said received captured information by said subscriber account provider utilizing a public key of said transaction processing device in order to verify the source of said received captured information.

14. The method of claim 13, wherein said received captured information is further decrypted utilizing the private key of a payment processor.

15. The method of claim 13, further comprising the step of:
providing at least a portion of said decrypted information to a third party server; and
receiving said verifying information from said third party server in response to providing said decrypted information to said third party server.

16. The method of claim 13, further comprising the step of:
retrieving, by said subscriber account provider, verifying information from said remote server, wherein said verifying information had been previously retrieved by said subscriber account provider from a third party server.

17. The method of claim 5, wherein said identifying information is received by said transaction processing device by scanning a card across a card reader associated with said transaction processing device.

18. The method of claim 17, wherein said card reader is part of said transaction processing device.

19. The method of claim 1, wherein said captured information is a driver's license number.

20. The method of claim 1, wherein said captured information is provided to said subscriber by a provider of said transaction processing device.

21. The method of claim 2, wherein said certifying authority provides independent verification of said subscriber based in part on said initial information.

22. The method of claim 1, further comprising the step of:
activating said transaction processing device for performing said network service upon successful verification of said subscriber.

23. The method of claim 1, further comprising the step of:
activating said subscriber account for providing said network service upon successful verification of said subscriber.

24. The method of claim 1, further comprising the step of:
activating said subscriber account for providing said network service upon successful verification of said subscriber and said transaction processing device.

25. The method of claim 23, wherein said activating step comprises the step of:
associating said subscriber account with said transaction processing device; and
enabling said subscriber account.

26. The method of claim 25, further comprising the step of:
transmitting data back to said transaction processing device.
27. The method of claim 26, wherein said transmitted data is configuration data.
28. The method of claim 1, wherein said network service is a payment processing service.
29. The method of claim 1, wherein said payment processing service includes credit card processing.
30. The method of claim 28, wherein said payment processing service is selected from the group consisting of debit card processing, check verification, check guarantee, payroll processing, gift certificate issuance, issuance of electronic tickets, and issuance of money order.
31. The method of claim 1, wherein said initial information is provided to a payment processor by said subscriber by entering information at a web site maintained by said payment processor.
32. The method of claim 31, wherein said information is entered by said subscriber via a wireless device.
33. The method of claim 1, wherein said transaction processing device is a standalone internet enabled transaction processing device.
34. The method of claim 1, wherein said transaction processing device is a standalone internet enabled wireless transaction processing device.
35. The method of claim 1, further comprising the step of:
providing by a provider of said subscriber account an identifying token to said subscriber separate from said transaction processing device.
36. The method of claim 35, wherein said identifying token is a username and a password.

37. The method of claim 35, wherein said identifying token is provided to said subscriber electronically in response to receiving said initial information from said subscriber.

38. The method of claim 35, wherein said identifying token is selected by said subscriber.

39. The method of claim 35, wherein said identifying token is selected by a provider of said subscriber account.

40. The method of claim 35, wherein said identifying token is encoded in a physical device provided to said subscriber by a provider of said subscriber account.

41. The method of claim 35, wherein said received captured information includes said identifying token that had been previously provided to said subscriber by said subscriber account provider.

42-47. (Cancelled)

48. A method for electronic authentication of a subscriber requesting a subscriber account for providing a payment processing service, comprising the steps of:

receiving initial information from said subscriber, wherein said initial information is received by a payment processor;

storing said received information in a database associated with said payment processor;

providing a point of sale terminal to said subscriber;

receiving by said point of sale terminal identifying information from said subscriber, wherein said identifying information is captured by said transaction processing device, wherein at least a portion of said captured information is encrypted by said point of sale terminal;

receiving said encrypted information from said point of sale terminal via a public network;

decrypting said received encrypted information by said payment processor;

providing at least a portion of said decrypted information to a third party server;

receiving verifying information from said third party server wherein said verifying information is related to said decrypted information provided to said third party server;

comparing said verifying information with said initial information by said payment processor to authenticate said subscriber; and

activating said subscriber account for performing said payment processing service upon authentication of said subscriber.

49. The method of claim 48, wherein said point of sale terminal utilizes a private key unique to said point of sale terminal for said encryption of said captured information.

50. The method of claim 49, wherein said payment processor utilizes a public key of said point of sale terminal for said decryption of said received encrypted information.

51-55. (Cancelled)

56. A method of activating a subscriber account for providing a network service via a transaction processing device, comprising:

- receiving initial information from a subscriber;
- storing said initial information;
- providing said transaction processing device to said subscriber;
- receiving identification information from said subscriber through said transaction processing device;
- communicating, by said transaction processing device through a network, said identification information to an authenticating server;
- using, by said authenticating server, said identification information to obtain verifying information related to said subscriber; and
- activating, by said authenticating server, said subscriber account when said verifying information is consistent with said initial information, wherein said activating enables said transaction processing device to initiate payments into said subscriber account from third parties via said network.

57. The method of claim 56 further comprising:
retrieving said verifying information through a third party server.

58. The method of claim 57 wherein said identification information is driver's license information and said retrieving communicates said driver's license information to said third party server to obtain said verifying information.

59. The method of claim 57 further comprising:
communicating at least one challenge question from said authenticating server to said subscriber through said transaction processing device as a condition to said activating.

60. The method of claim 56 further comprising:
verifying an identifier of said transaction processing device by said authenticating server as a condition to said activating.

61. The method of claim 56 wherein said activating comprises:
communicating configuration information to said transaction processing device.

IX. EVIDENCE

Not Applicable.

X. RELATED PROCEEDINGS

Not Applicable.